OCR Issues Fact Sheet on Direct Liability for Business Associates under HIPAA

September 25, 2019

HHS's Office for Civil Rights(?ÃÂ£OCR?ÃÂ¥), which is the government agency responsible for enforcement of the HIPAA privacy, security, breach notification, and enforcement rules (the ?ÃÂ£HIPAA Rules?ÃÂ¥), recently issued a new fact sheet (?ÃÂ£Fact Sheet?ÃÂ¥). The Fact Sheet recaps the provisions in the HIPAA Rules for which a HIPAA business associate may be held directly liable for compliance. HIPAA business associates of an employer-sponsored group health plan, which is a ?ÃÂ£covered entity?ÃÂ¥ under HIPAA, would include, for example, the health plan?ÃÃs third-party claims administrator, a health plan consulting firm, a benefits broker, and the health plan?ÃÃs outside legal counsel, if such persons or entities create, receive, maintain, or transmit HIPAA protected health information (?ÃÂ£PHI?ÃÂ¥) on behalf of the health plan.

The Fact Sheet clarified that OCR has authority to take enforcement action against business associates only for certain requirements and prohibitions of the HIPAA Rules as listed in the Fact Sheet, including, without limitation:

?ÃÃ³ Failure to comply with the requirements of the HIPAA security rule; ?ÃÃ³ Failure to provide breach notification to a covered entity, such as an employer-sponsored group health plan, or another business associate; ?ÃÃ³ Impermissible uses and disclosures of PHI;

?ÃÃ³ Failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request;

?ÃÃ³ Failure to enter into business associate agreements with their subcontractors that create or receive PHI on their behalf, and failure to comply with the implementation specifications for such agreements; and

?ÃÃ³ Failure to take reasonable steps to address a material breach or violation of the subcontractor?ÃÃs business associate agreement.

In today's business environment, employers outsource many aspects of health plan administration to their business associates. The Fact Sheet serves as an important reminder to employers that business associates are not directly subject under the HIPAA Rules to all the requirements that apply to employer-sponsored group health plans.

Employers cannot outsource to business associates certain obligations under the HIPAA Rules with immunity from liability. For example, business associates are not directly responsible under the HIPAA Rules for the issuance and administration of required notifications to individuals, the media (in some cases), and HHS when a breach of unsecured PHI occurs, regardless of whether the business associate (or its subcontractor) is the party that commits the breach. Instead, such notification obligations remain with the health plan.

A copy of the fact sheet is available here.